

EXAMPLES OF PLANE RATIONAL CURVES WITH TWO GALOIS POINTS IN POSITIVE CHARACTERISTIC

SATORU FUKASAWA AND KATSUSHI WAKI

ABSTRACT. We present four new examples of plane rational curves with two Galois points in positive characteristic, and determine the number of Galois points for three of them. Our results are related to a problem on projective linear groups.

1. INTRODUCTION

Let $C \subset \mathbb{P}^2$ be an irreducible plane curve over an algebraically closed field k of characteristic $p \geq 0$ with $k(C)$ as its function field. For a point $P \in \mathbb{P}^2$, if the function field extension $k(C)/\pi_P^*k(\mathbb{P}^1)$ induced by the projection π_P is Galois, then P is called a Galois point for C . This notion was introduced by Yoshihara ([4, 6]). Furthermore, if a Galois point P is a smooth point of C (resp. a point in $\mathbb{P}^2 \setminus C$), then P is said to be inner (resp. outer). The associated Galois group at P is denoted by G_P . Determining the number of Galois points in general is difficult. For example, there are not so many examples of plane curves with two Galois points (see the Tables in [8]). In this note, we present four examples of plane rational curves with two Galois points, which update the Tables in [8].

Hereafter, we assume that $p \geq 3$ and $q \geq 5$ is a power of p .

Theorem 1. *Let C_1 be the plane curve of degree q which is the image of the morphism*

$$\varphi_1 : \mathbb{P}^1 \rightarrow \mathbb{P}^2; (s : t) \mapsto (s^{\frac{q+1}{2}} t^{\frac{q-1}{2}} : (s-t)t^{q-1} : s^q - st^{q-1}).$$

Then:

- (a) *The point $P_1 := (0 : 1 : 0) = \varphi_1(0 : 1)$ is an inner Galois point with $G_{P_1} \cong D_{q-1}$, where D_{q-1} is the dihedral group of order $q-1$.*
- (b) *The point $P_2 := (1 : 0 : 0) = \varphi_1(1 : 1)$ is an inner Galois point with $G_{P_2} \cong \mathbb{Z}/(q-1)\mathbb{Z}$.*

2010 *Mathematics Subject Classification.* 14H50, 20G40.

Key words and phrases. Galois point, plane curve, Galois group, projective linear groups.

The first author was partially supported by JSPS KAKENHI Grant Number 16K05088.

(c) *The number of inner Galois points on C_1 is exactly two.*

Theorem 2. *Let C_2 be the plane curve of degree q which is the image of the morphism*

$$\varphi_2 : \mathbb{P}^1 \rightarrow \mathbb{P}^2; (s : t) \mapsto (s^{\frac{q+1}{2}} t^{\frac{q-1}{2}} : (s-t)^{\frac{q+1}{2}} t^{\frac{q-1}{2}} : s^q - st^{q-1}).$$

Then:

- (a) *The point $P_1 := (0 : 1 : 0) = \varphi_2(0 : 1)$ is an inner Galois point with $G_{P_1} \cong D_{q-1}$.*
- (b) *The point $P_2 := (1 : 0 : 0) = \varphi_2(1 : 1)$ is an inner Galois point with $G_{P_2} \cong D_{q-1}$.*
- (c) *The number of inner Galois points on C_2 is exactly two.*

For the case where the characteristic is zero and C is rational, Yoshihara [7, Lemma 13] asserts that cyclic and dihedral groups do not appear as Galois groups of outer Galois points at the same time. To the contrary, in positive characteristic, we present the following example.

Theorem 3. *Let C_3 be the plane curve of degree $q+1$ which is the image of the morphism*

$$\varphi_3 : \mathbb{P}^1 \rightarrow \mathbb{P}^2; (s : t) \mapsto (s^{\frac{q+1}{2}} t^{\frac{q+1}{2}} : (s+t)^{q+1} : s^{q+1} + \gamma t^{q+1}),$$

where $\gamma \in \mathbb{F}_q \setminus \{0, \pm 1\}$. Then:

- (a) *The point $P_1 := (0 : 1 : 0)$ is an outer Galois point with $G_{P_1} \cong D_{q+1}$.*
- (b) *The point $P_2 := (1 : 0 : 0)$ is an outer Galois point with $G_{P_2} \cong \mathbb{Z}/(q+1)\mathbb{Z}$.*
- (c) *The number of outer Galois points for C_3 is exactly two.*

Theorem 4. *Let C_4 be the plane curve of degree $q+1 > 6$ which is the image of the morphism*

$$\varphi_4 : \mathbb{P}^1 \rightarrow \mathbb{P}^2; (s : t) \mapsto (s^{\frac{q+1}{2}} t^{\frac{q+1}{2}} : (s+t)^{\frac{q+1}{2}} (s+\gamma t)^{\frac{q+1}{2}} : s^{q+1} - \gamma t^{q+1}),$$

where $\gamma \in \mathbb{F}_q \setminus \{\pm 1\}$ and $\gamma^{\frac{q-1}{2}} = 1$. Then:

- (a) *The point $P_1 := (0 : 1 : 0)$ is an outer Galois point with $G_{P_1} \cong D_{q+1}$.*
- (b) *The point $P_2 := (1 : 0 : 0)$ is an outer Galois point with $G_{P_2} \cong D_{q+1}$.*

Our results are closely related to the following problem on projective linear groups (cf. [2, Theorem 1]).

Problem 1. Let k be a field and $X = \mathbb{P}^1(k)$ the projective line over k . We consider the following two conditions for a pair (H_1, H_2) of different finite subgroups H_1 and $H_2 \subset \text{PGL}(2, k)$:

- (a) $H_1 \cap H_2 = \{1\}$.
- (b) There exist different points P_1 and $P_2 \in X$ such that

$$\{\sigma(P_2) \mid \sigma \in H_1 \setminus \{1\}\} = \{\tau(P_1) \mid \tau \in H_2 \setminus \{1\}\}$$

(with multiplicities).

When does a pair (H_1, H_2) with (a) and (b) exist?

2. PROOF OF THEOREMS 1 AND 2

We assume that $\alpha \in \mathbb{F}_q$ is a primitive element. The following two lemmas are easily proved.

Lemma 1. Let σ and $\tau \in \text{Aut}(\mathbb{P}^1) \cong \text{PGL}(2, k)$ be represented by the matrices

$$A_\sigma = \begin{pmatrix} 1 & 0 \\ 0 & \alpha^2 \end{pmatrix} \quad \text{and} \quad A_\tau = \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix}$$

respectively, that is, $\sigma(s, t) = (s, t)A_\sigma$ and $\tau(s, t) = (s, t)A_\tau$. Then:

- (a) The group H generated by σ and τ is isomorphic to D_{q-1} .
- (b) The rational function $f(s) = s^{\frac{q-1}{2}} - s^{-\frac{q-1}{2}} \in k(\mathbb{P}^1) = k(s)$ is invariant under the action by H .

Lemma 2. Let $\eta \in \text{Aut}(\mathbb{P}^1)$ be represented by the matrix

$$A_\eta = \begin{pmatrix} 1 & 0 \\ \alpha - 1 & \alpha \end{pmatrix}.$$

Then:

- (a) The order of η is $q - 1$.
- (b) The rational function $g(s) = \frac{s-1}{s^q-s} \in k(\mathbb{P}^1) = k(s)$ is invariant under the action by η^* .

When R_1 and R_2 are different points in \mathbb{P}^2 , the line passing through R_1 and R_2 is denoted by $\overline{R_1 R_2}$.

Proof of Theorem 1. The composite (rational) map $\pi_{P_1} \circ \varphi_1$ is given by

$$(s : t) \mapsto (s^{\frac{q+1}{2}} t^{\frac{q-1}{2}} : s^q - s t^{q-1}) = (s^{\frac{q-1}{2}} t^{\frac{q-1}{2}} : s^{q-1} - t^{q-1}),$$

since π_{P_1} is represented by $(X : Y : Z) \mapsto (X : Z)$. By this expression, the degree of $\pi_{P_1} \circ \varphi_1$ is $q - 1$ and hence, φ_1 is birational onto the image C_1 . Note that

$$\pi_{P_1} \circ \varphi_1(s : 1) = \left(s^{\frac{q-1}{2}} : s^{q-1} - 1 \right) = (1 : f(s)),$$

where $f(s)$ is the rational function as in Lemma 1. By Lemma 1, the rational function $f(s)$ is invariant under the action by $H \cong D_{q-1}$. Therefore, $k(s)/k(f(s))$ is a Galois extension and hence, P_1 is a Galois point. In this case, $G_{P_1} \cong D_{q-1}$. Assertion (a) in Theorem 1 follows. Further,

$$\pi_{P_2} \circ \varphi_1(s : 1) = (s - 1 : s^q - s) = (g(s) : 1),$$

where $g(s)$ is the rational function as in Lemma 2. By Lemma 2, the rational function $g(s)$ is invariant under the action by η^* . Therefore, $k(s)/k(g(s))$ is a Galois extension and hence, P_2 is a Galois point. In this case, $G_{P_2} \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Assertion (b) in Theorem 1 follows.

We prove that the set of all inner Galois points for C_1 is equal to $\{P_1, P_2\}$. Let $Q := \varphi_1(1 : 0) = (0 : 0 : 1)$. Then, the composite map $\pi_Q \circ \varphi_1$ is given by

$$(s : t) \mapsto (s^{\frac{q+1}{2}} t^{\frac{q-1}{2}} : (s - t)t^{q-1}) = (s^{\frac{q+1}{2}} : (s - t)t^{\frac{q-1}{2}}).$$

Since the degree of $\pi_Q \circ \varphi_1$ is $(q+1)/2$, the point Q is a singular point of C_1 with multiplicity $(q-1)/2$. The ramification indices of $\pi_Q \circ \varphi_1$ at $(0 : 1)$ and at $(1 : 0)$ are equal to $(q+1)/2$ and $(q-1)/2$ respectively. For the function $h(t) = (1-t)t^{\frac{q-1}{2}}$,

$$h'(t) = -\frac{1}{2}t^{\frac{q-3}{2}}(1+t).$$

Therefore, three points $(0 : 1)$, $(1 : 0)$ and $(1 : -1)$ are all ramification points for $\pi_Q \circ \varphi_1$. Furthermore, the ramification index at $(1 : -1)$ is 2. Note that $\varphi_1^{-1}(Q)$ consists of a unique point $(1 : 0)$. Therefore, for each point $R \in C_1 \setminus \{Q\}$, the map $\pi_R \circ \varphi_1$ is ramified at $(1 : 0)$ with index $\geq (q-1)/2$. Assume that R is an inner Galois point. It follows from [5, III. 7.2] that $\pi_R \circ \varphi_1$ is ramified at $(1 : 0)$ with index $(q-1)/2$ or $q-1$. If the index at $(1 : 0)$ is $q-1$, then $R = P_2$. Assume that the index at $(1 : 0)$ is $(q-1)/2$. Then, there exists a ramification point $\hat{S} \in \mathbb{P}^1$ with index $(q-1)/2$ such that $\varphi_1(\hat{S}) \neq Q$ and $\varphi_1(\hat{S}) \in \overline{RQ}$. Considering $\pi_Q \circ \varphi_1$, $\hat{S} = (0 : 1)$ or $(1 : -1)$. If $\hat{S} = (0 : 1)$, then $R = \varphi_1(0 : 1) = P_1$, since $C_1 \cap \overline{P_1Q} = \{P_1, Q\}$. Assume that $\hat{S} = (1 : -1)$. Then, $(q-1)/2 = 2$, and hence, $q = 5$ and $R \in \overline{Q\varphi_1(1 : -1)}$. However, this is a contradiction, because the point $\varphi_1(1 : -1) = (1 : 2 : 0) = \varphi_1(2 : 1)$ is a

singular point and $C \cap \overline{Q\varphi_1(1 : -1)} = \{Q, \varphi_1(1 : -1)\}$. We complete the proof of Theorem 1(c). \square

Proof of Theorem 2. Assertion (a) in Theorem 2 is similar to assertion (a) in Theorem 1. The composite map $\pi_{P_2} \circ \varphi_2$ is given by

$$(s : 1) \mapsto ((s - 1)^{\frac{q+1}{2}} : s^q - s) = (1 : f(s - 1)).$$

Then, the induced field extension is $k(u)/k(f(u))$, where $u = s - 1$. This is a Galois extension, similar to assertion (a) in Theorem 1. Assertion (b) in Theorem 2 follows.

We prove that the set of all inner Galois points for C_2 is equal to $\{P_1, P_2\}$. Let $Q := \varphi_2(1 : 0) = (0 : 0 : 1)$. Then, the composite map $\pi_Q \circ \varphi_2$ is given by

$$(s : t) \mapsto (s^{\frac{q+1}{2}} t^{\frac{q-1}{2}} : (s - t)^{\frac{q+1}{2}} t^{\frac{q-1}{2}}) = (s^{\frac{q+1}{2}} : (s - t)^{\frac{q+1}{2}}).$$

Since the degree of $\pi_Q \circ \varphi_2$ is $(q + 1)/2$, the point Q is a singular point of C_2 with multiplicity $(q - 1)/2$. Further, by this expression, $\pi_Q \circ \varphi_2$ is a cyclic covering and all ramification points are $(0 : 1)$ and $(1 : 1)$ with index $(q + 1)/2$. Note that $\varphi_2^{-1}(Q)$ consists of a unique point $(1 : 0)$, and the intersection multiplicity of $C_2 \cap L$ at Q is at most $\frac{q-1}{2} + 1$ for any line L passing through Q . Therefore, for each point $R \in C_2 \setminus \{Q\}$, the map $\pi_R \circ \varphi_2$ is ramified at $(1 : 0)$ with index $(q - 1)/2$ or $(q + 1)/2$. Assume that R is an inner Galois point. It follows from [5, III. 7.2] that $\pi_R \circ \varphi_2$ is ramified at $(1 : 0)$ with index $(q - 1)/2$. Then, there exists a ramification point $\hat{S} \in \mathbb{P}^1$ with index $(q - 1)/2$ such that $\varphi_2(\hat{S}) \neq Q$ and $\varphi_2(\hat{S}) \in \overline{RQ}$. Considering $\pi_Q \circ \varphi_2$, $\hat{S} = (0 : 1)$ or $(1 : 1)$. Then, $R = P_1$ or P_2 , since $C_2 \cap \overline{QP_i} = \{Q, P_i\}$ for $i = 1, 2$. We complete the proof of Theorem 2(c). \square

3. PROOF OF THEOREMS 3 AND 4

Proof of Theorem 3. Let $Q := \varphi_3(1 : 0) = (0 : 1 : 1)$. Then, the composite map $\pi_Q \circ \varphi_3$ is given by

$$(s : t) \mapsto (s^{\frac{q+1}{2}} t^{\frac{q-1}{2}} : (s + t)^{q+1} - (s^{q+1} + \gamma t^{q+1})) = (s^{\frac{q+1}{2}} t^{\frac{q-1}{2}} : s^q + st^{q-1} + (1 - \gamma)t^q).$$

Since $\gamma \neq 1$, the degree of $\pi_Q \circ \varphi_3$ is q and hence, φ_3 is birational onto the image C_3 .

We consider the point P_1 . Since $\gamma \neq 0$, $P_1 \in \mathbb{P}^2 \setminus C_3$. The composite map $\pi_{P_1} \circ \varphi_3$ is given by

$$(s : 1) \mapsto (s^{\frac{q+1}{2}} : s^{q+1} + \gamma) = (1 : s^{\frac{q+1}{2}} + \gamma s^{-\frac{q+1}{2}}).$$

The rational function $s^{\frac{q+1}{2}} + \gamma s^{-\frac{q+1}{2}}$ is invariant under the actions $s \mapsto \delta s^{-1}$ and $s \mapsto \zeta s$, where δ is a $(q+1)/2$ -th root of γ and ζ is a $(q+1)/2$ -th root of unity. Therefore, the extension $k(\mathbb{P}^1)/\pi_{P_1}^* k(\mathbb{P}^1)$ is a Galois extension and hence, P_1 is a Galois point. In this case, $G_{P_1} \cong D_{q+1}$. Assertion (a) in Theorem 3 follows. We consider the point P_2 . Since $\gamma \neq -1$, $P_2 \in \mathbb{P}^2 \setminus C_3$. The composite map $\pi_{P_2} \circ \varphi_3$ is given by

$$(s : 1) \mapsto ((s+1)^{q+1} : s^{q+1} + \gamma).$$

Note that

$$(1 + \gamma)(s^{q+1} + \gamma) - \gamma(s+1)^{q+1} = (s - \gamma)^{q+1}.$$

Therefore, the extension $k(\mathbb{P}^1)/\pi_{P_2}^* k(\mathbb{P}^1)$ is a Galois extension and hence, P_2 is a Galois point. In this case, $G_{P_2} \cong \mathbb{Z}/(q+1)\mathbb{Z}$. Assertion (b) in Theorem 3 follows.

We prove that the set of all outer Galois points for C_3 is equal to $\{P_1, P_2\}$. Note that the rank of the matrix

$$\begin{pmatrix} \varphi_3 \\ \frac{d\varphi_3}{ds} \end{pmatrix} = \begin{pmatrix} s^{\frac{q+1}{2}} & (s+1)^{q+1} & s^{q+1} + \gamma \\ \frac{q+1}{2}s^{\frac{q-1}{2}} & (s+1)^q & s^q \end{pmatrix}$$

is two for each s , that is, the differential map of φ_3 is injective at each point $(s : 1) \in \mathbb{P}^1$. We consider the Hessian matrix H of φ_3 :

$$\begin{pmatrix} \varphi_3 \\ \frac{d\varphi_3}{ds} \\ \frac{d^2\varphi_3}{ds^2} \end{pmatrix} = \begin{pmatrix} s^{\frac{q+1}{2}} & (s+1)^{q+1} & s^{q+1} + \gamma \\ \frac{q+1}{2}s^{\frac{q-1}{2}} & (s+1)^q & s^q \\ \frac{q^2-1}{4}s^{\frac{q-3}{2}} & 0 & 0 \end{pmatrix}.$$

Note that $\det H = 0$ if and only if $s = 0, -1, \gamma$. It follows that all flexes of C_3 are $(1 : 0), (0 : 1), (-1 : 1)$ and $(\gamma : 1)$ (see [3, Section 7.6]). If R is an outer Galois point such that the order of G_R is at least five, then there exists a ramification point with index at least three (see, for example, [3, Theorem 11.91]). Then, R is contained in the tangent line at a flex. If $R \neq P_2$, then R is contained in the line defined by $X = 0$, which passes through points $\varphi_3(1 : 0), \varphi_3(0 : 1)$ and P_1 . It follows from [5, III. 7.2, 8.2] that there exist subgroups $H_1 \subset G_{P_1}$ and $H_2 \subset G_R$ of order $\frac{q+1}{2}$ fixing the point $(1 : 0)$. Then, H_1 and H_2 are normal subgroups of G_{P_1} and G_R respectively, and hence, they fix points $(1 : 0)$ and $(0 : 1)$. By a property of $\text{PGL}(2, k)$, it follows that $H_1 = H_2$, that is, $G_{P_1} \cap G_R \neq \{1\}$. This is a contradiction (see, for example, [1, Lemma 7]). We complete the proof of Theorem 3. \square

Proof of Theorem 4. Let $Q := \varphi_4(1 : 0) = (0 : 1 : 1)$. Then, the composite map $\pi_Q \circ \varphi_4$ is given by

$$(s : t) \mapsto (s^{\frac{q+1}{2}} t^{\frac{q+1}{2}} : (s+t)^{\frac{q+1}{2}} (s+\gamma t)^{\frac{q+1}{2}} - (s^{q+1} - \gamma t^{q+1})).$$

Note that the coefficient of t^{q+1} and $s^q t$ for the function $(s+t)^{\frac{q+1}{2}} (s+\gamma t)^{\frac{q+1}{2}} - (s^{q+1} - \gamma t^{q+1})$ is $\gamma^{\frac{q+1}{2}} + \gamma = 2\gamma \neq 0$ and $\frac{q+1}{2}(\gamma+1) \neq 0$ respectively. The degree of $\pi_Q \circ \varphi_3$ is q and hence, φ_4 is birational onto the image C_4 .

We consider the point P_1 . Since $\gamma \neq 0$, $P_1 \in \mathbb{P}^2 \setminus C_4$. The composite map $\pi_{P_1} \circ \varphi_4$ is given by

$$(s : 1) \mapsto (s^{\frac{q+1}{2}} : s^{q+1} - \gamma) = (1 : s^{\frac{q+1}{2}} - \gamma s^{-\frac{q+1}{2}}).$$

The rational function $s^{\frac{q+1}{2}} - \gamma s^{-\frac{q+1}{2}}$ is invariant under the actions $s \mapsto \delta s^{-1}$ and $s \mapsto \zeta s$, where δ is a $(q+1)/2$ -th root of $-\gamma$ and ζ is a $(q+1)/2$ -th root of unity. Therefore, the extension $k(\mathbb{P}^1)/\pi_{P_1}^* k(\mathbb{P}^1)$ is a Galois extension and hence, P_1 is a Galois point. In this case, $G_{P_1} \cong D_{q+1}$. Assertion (a) in Theorem 4 follows. We consider the point P_2 . Since $(-1)^{q+1} - \gamma \neq 0$ and $(-\gamma)^{q+1} - \gamma = \gamma(\gamma-1)^q \neq 0$, it follows that $P_2 \in \mathbb{P}^2 \setminus C_4$. The composite map $\pi_{P_2} \circ \varphi_4$ is given by

$$(s : 1) \mapsto ((s+1)^{\frac{q+1}{2}} (s+\gamma)^{\frac{q+1}{2}} : s^{q+1} - \gamma).$$

Note that

$$\frac{1}{1-\gamma} \{-\gamma(s+1)^{q+1} + (s+\gamma)^{q+1}\} = s^{q+1} - \gamma.$$

Let

$$u := \frac{s+\gamma}{s+1} \quad \text{and} \quad h(u) := -\gamma u^{-\frac{q+1}{2}} + u^{\frac{q+1}{2}}.$$

Then, $k(\mathbb{P}^1)/\pi_{P_2}^* k(\mathbb{P}^1) = k(u)/k(h(u))$. This is a Galois extension, similar to assertion (a) in Theorem 4. In this case, $G_{P_2} \cong D_{q+1}$. Assertion (b) in Theorem 4 follows. \square

REFERENCES

- [1] S. Fukasawa, Classification of plane curves with infinitely many Galois points, J. Math. Soc. Japan **63** (2011), 195–209.
- [2] S. Fukasawa, A birational embedding of an algebraic curve into a projective plane with two Galois points, preprint, arXiv:1611.03953.
- [3] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic curves over a finite field*, Princeton Univ. Press, Princeton, 2008.
- [4] K. Miura and H. Yoshihara, Field theory for function fields of plane quartic curves, J. Algebra **226** (2000), 283–294.
- [5] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

- [6] H. Yoshihara, Function field theory of plane curves by dual curves, J. Algebra **239** (2001), 340–355.
- [7] H. Yoshihara, Galois points for plane rational curves, Far East J. Math. **25** (2007), 273–284; Errata, ibid. **29** (2008), 209–212.
- [8] H. Yoshihara and S. Fukasawa, List of problems, available at:
<http://hyoshihara.web.fc2.com/openquestion.html>

DEPARTMENT OF MATHEMATICAL SCIENCES, FACULTY OF SCIENCE, YAMAGATA UNIVERSITY,
KOJIRAKAWA-MACHI 1-4-12, YAMAGATA 990-8560, JAPAN

E-mail address: `s.fukasawa@sci.kj.yamagata-u.ac.jp`

E-mail address: `waki@sci.kj.yamagata-u.ac.jp`